Vysoká škola báňská – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Mobilní telefon a šifrovaný provoz

Encrypted Traffic of Smartphone

2014/15

Petr Pospíšil

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání bakalářské práce

Student: **Petr Pospíšil**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2612R059 Mobilní technologie

Téma: Mobilní telefón a šifrovaný provoz
Encrypted Traffic of Smartphone

Zásady pro vypracování:

Jednou z možnosti úniku informací je odposlech hovoru z mobilního telefonu. K omezení úniku se používají jednak speciální šifrované mobily nebo dodatečně instalované programy do chytrých mobilů. V oblasti chytrých mobilních telefonu převládá operační systém Android.

Cílem práce je popsat možnosti šifrování hovorů v mobilních telefonech a navrhnout, realizovat šifrovaný provoz mezi dvěma mobilními telefony.

Práce bude obsahovat
- Popis šifrovaní telefonních hovorů
- Výběr vhodného programového vybavení pro šifrovaný hovor
- Návrh experimentu a jeho uskutečnění
- Vyhodnocení experimentu

Seznam doporučené odborné literatury:

- Keith M. Martin: Everyday Cryptography: Fundamental Principles and Applications; Oxford University Press 2012, ISBN-13: 978-0199695591
- Christof Paar, Jan Pelzl, Bart Preneel: Understanding Cryptography: A Textbook for Students and Practitioners; Springer 2010, ISBN-13: 978-3642041006

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **doc. Ing. Jaroslav Zdrálek, Ph.D.**

Datum zadání: 01.09.2014
Datum odevzdání: 07.05.2015

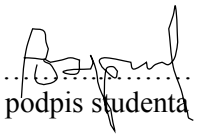
doc. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne: *30. dubna 2015*



podpis studenta

Poděkování

Rád bych poděkoval panu doc. Ing. Jaroslavu Zdrálkovi, Ph.D. za rady ohledně tvorby této práce. Dále bych také poděkoval panu Ing. Romanu Šebestovi, Ph.D. za zapůjčení vybavení k měření.

Abstrakt

Cílem této práce je nalezení vhodných aplikací pro šifrovaný, bezpečný přenos informací skrze mobilní telefony. Protože samotná GSM síť je zranitelná, jak je v práci popsáno, k přenosu dat byl zvolen jiný kanál, a to datové přenosy skrze VoIP telefonii. Ta poskytuje nové možnosti zabezpečení. Bude vysvětleno jak VoIP funguje a na kterých technologiích nejčastěji pracuje. Dále bude představeno několik dalších užitečných aplikací pro šifrované psaní zpráv, instant messaging a utajení identity na Internetu. Hlavní části práce bude otestování freeware aplikací pro VoIP pro Android, jejich následné srovnání. Tyto aplikace budou taktéž srovnány s komerčním řešením.

Klíčová slova

Zabezpečení GSM; VoIP; Android; Ostel; RedPhone; SIP; ZRTP; SIM karty, A5/1;

Abstract

The goal of this task is to find suitable applications for ciphered, secure transmission of information through mobile phones. Because the GSM itself is vulnerable, as written in thesis, for data transmission was chosen different channel, data transmission through VoIP. This offers new options of security. There will be found out how VoIP works and most technologies which VoIP uses the most. There are presented next useful applications for encrypted text messaging, instant messaging and hiding identity in the Internet. The main goal of this thesis is testing of freeware applications for VoIP on Android platform. Then they will be compared. Also there will be compared freeware and commercial solution.

Key words

GSM security; VoIP; Android; Ostel; RedPhone; SIP; ZRTP; SIM cards, A5/1;

Seznam použitých zkratek

Zkratka	Význam
AES	Advanced Encryption Standard
BTS	Base transceiver station
DES	Data Encryption Standard
D-H	Diffie–Hellman key exchange
EAL4	Evaluation Assurance Level
EDGE	Enhanced Data rates for GSM Evolution
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GSMAi	GSMA Intelligence
HSPA	High Speed Packet Access
HTTP	Hypertext Transfer Protocol
ICCID	Universal Integrated Circuit Card
IIN	Issuer identification number
IMSI	International mobile subscriber identity
Ki	Authentication key
LAI	Location area identity
LTE	Long-Term Evolution
MOS	Mean opinion score
OTR	Off-the-Record Messaging
RTP	Real-time Transport Protocol
RTT	Round-trip time
SHA-1	Secure hash algorithm
SIM	Subscriber identity module
SIP	Session Initiation Protocol
SRES	Signed Response

SRTP	Secure Real-time Transport Protocol
TCP	Transmission Control Protocol
TGP	The Guardian Project
TLS	Transport Layer Security
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
VoIP	Voice over Internet Protocol
WAP	Wireless Application Protocol
ZRTP	Zimmermann Real-time Transport Protocol

Obsah

Úvod

Hlavním tématem této práce je průzkum a testování freeware aplikací určených k zabezpečení mobilních hovorů vůči odposlechům.

První kapitole práce obsahuje základní informace o šifrování, přináší základní představu o šifrování obecně. V druhé části je rozebráno, jak funguje samotné GSM a jeho zabezpečení. Jsou zde nastíněny jeho nedostatky a možnosti jak tyto nedostatky využít k prolomení šifrování.

Cílem druhé kapitoly bude seznámení se s aktuálně nejpoužívanější formou zabezpečení telefonních hovorů a to využití VoIP. Bude vysvětleno jak VoIP funguje, jaké technologie využívá. V druhá část obsahuje seznámení s aktuálními možnostmi zabezpečení. A to jak v komerčním sektoru, tak především na poli open source aplikací.

Poslední třetí část obsahuje výběr testovaných aplikací, jejich měření na dvou různých připojení a následné vyhodnocení testování a doporučení pro případné zájemce o zabezpečení jejich dat v mobilním telefonu.

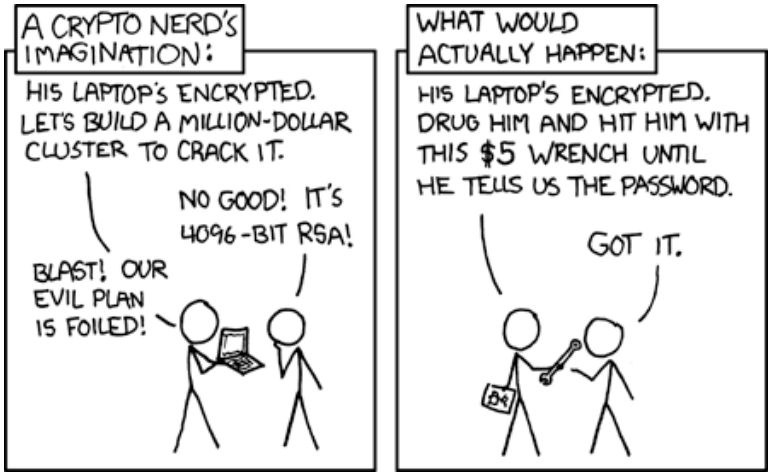
1 Úvod do kryptografie

V této části si nejdříve řekneme ve zkratce základní informace o šifrování. Vysvětlíme si co vlastně ona šifra je, jaké jsou její druhy a jak je zlomit. Dále bude následovat stručný popis šifer, část o GSM a jeho zabezpečení.

1.1 Co je to šifra?

Šifra neboli šifrovaná zpráva jsou výstupní data, po použití kryptografického algoritmu na text otevřeny, tj. původní text, který chceme skrýt. Slovo kryptografie[2] má základ v řeckém slově „krypós“ – skrytý či tajemství a „gráphein“ – psát.

Kryptografie samotná se dělí do 2 hlavních větví. Do klasické kryptografie a do kryptografie moderní. Jako konec klasické a začátek moderní kryptografie je většinou považováno období 2. světové války, kdy se k šifrování zpráv začaly používat první stroje, mezi které patří slavná Enigma. Začátek éry moderní kryptografie[2] se tedy dá zasadit do 50. let 20. století, kdy se ke slovu začaly dostávat první počítače a šifrování využívalo složitější a složitější algoritmy, jejichž implementaci počítače umožňovaly.



Obrázek 1.1: Obecný problém dokonalého šifrování

1.2 Bezpečností cíle šifrování

Proč šifrujeme komunikaci? Čeho chceme dosáhnout, pokud sáhneme po moderních šifrovacích nástrojích? V následujících několika bodech shrnu základní cíle.

- **Důvěrnost dat –** jedná se o poskytnutí přístupu k informacím pro oprávněné uživatele. Naopak neoprávnění uživatelé k informacím přístup mít nesmějí. Za předpokladu, že informace jsou přenášeny na veřejném kanálu, je nutno zprávu zašifrovat.
- **Integrita dat –** neboli zajištění celistvosti dat, tj. data nebyly nijak změněny během přenosu. Nebyly zkráceny, prodlouženy.
- **Autentizace entit –** ověřuje avizovanou identitu, tzn., kontroluje, zda odesilatel např. uživatel bankovnictví je opravdu tím daným uživatelem, kdo je oprávněn k platbě a nejedná se o podvrhnutou identitu.
- **Autentizace dat –** ověřuje avizovanou identitu dat, tj. kontroluje např. metadata zprávy. Konkrétně ověřuje čas vytvoření, původ zprávy a podobně.
- **Nepopiratelnost –** zajišťuje, aby daný subjekt nemohl popřít to, co v minulosti vykonal. V následujících řádcích uvedu několik příkladů, se kterými se běžně potkáváme.
    - **Nepopiratelnost původu** – např. platba byla odeslána oprávněným uživatelem.
    - **Nepopiratelnost přenosu –** např. v minulosti potvrzovací SMS o doručení zprávy.
    - **Nepopiratelnost znalosti –** např. chatovací klient webové aplikace Facebook. Po přijetí zprávy a jejím přečtení je odesilatel informován o tom, že příjemce zprávu zpracoval.
- **Důvěryhodné vyznačení času**
- **Řízení přístupu –** jen oprávněné subjekty mají přístup k informacím, které jim jsou určeny.
- **Autorizace –** určitou činnost v systému může vykonávat pouze oprávněný uživatel.

1.3 Klasické šifry

Mezi klasické šifry[2] lze zařadit všechny způsoby kryptografie, které k zakódování původní zprávy využívají substituci, nebo transpozici znaků nebo skupiny znaků. Klasické šifry se využívaly především v minulosti. Mezi nejstarší patří například známa Caesarova šifra, která se používala mimo jiné také k šifrování vojenských depeší. Jedná se tedy o velmi starý a jednoduchý způsob skrytí informací.

Období klasických šifer začíná přibližně 1900 př.n.l. V těchto letech byla poprvé použita určitá primitivní forma „šifrování“ v Egyptě. Jednalo se o použití nestandartních znaků, hieroglyfů v rytinách. Tedy nejde o šifru v pravém slova smyslu skrývající tajemství, jako spíš určitá snaha o zmatení čtenáře a vzbuzení pozornosti.

Různé formy kódů se vyskytovali ve všech starověkých civilizacích. Jeden z nejstarších však byl nalezen v Mezopotámii. Jednalo se o jílovou tabulku. Na té bylo pomocí klínového písma zakódována informace. Forma kódování byla jednoduchá. Běžné znaky byly nahrazovány nestandartními, byly vynechávány první znaky slov a stejná slova měly různé psané podoby. A jaké tajemství tabulka skrývala? Návod na výrobu keramiky. Stáří tabulky odpovídá asi 3500 let. Ano, i v období 1500 př.n.l. existovala průmyslová špionáž.

1.3.1 Substituční šifrovací metoda

Jedná se o základní šifrovací metodu, používanou v minulosti. Dnes je velmi zastaralá a je velmi jednoduše prolomitelná i bez použití výpočetní techniky.

Princip substituční šifry[3][4] spočívá v nahrazení znaku za jiný znak. V praxi se mohou, pro větší účinnost, substituovat jednotlivé znaky za skupiny znaků a naopak.

Existuje několik různých druhů substitučních šifer na základě počtu šifrovaných znaků.

- **Jednoduchá substituční šifra** pracuje pouze se znaky. Mění právě jeden znak za jiný znak. Jedná se například o Caesarovu šifru a plno dalších šifer na podobném principu.
- **Polygrafická substituční šifra** pracuje s většími skupinami znaků. Lze zaměňovat n znaků za m znaků a podobně. Příkladem může být Hillova substituční šifra založena na znalosti lineární algebry.

1.3.2 Transpoziční šifrovací metoda

Základní rozdíl mezi substituční a transpoziční šifrou je takový, že v transpoziční šifře[3][5] jsou znakům pouze změněny pozice, tzn., že znaky v dešifrované zprávě budou naprosto stejné jako v šifrované. Pouze budou jinak rozmístěny. Výhodou této šifry je její jednoduchost a možnost použití bez znalostí matematiky. To jsou ale zároveň hlavní zápory. Pro její jednoduchost je riziko odhalení otevřeného textu výrazné, poněvadž lze použít frekvenční analýzy. V praxi se proto často kombinovala s jinými šiframi pro zvýšení síly šifry.

1.3.3 **Caesarova šifra**

Caesarova šifra[3] patří mezi nejznámější klasické šifry mezi laickou veřejností. Samotná šifra patří do kategorie substitučních šifer. Princip je jednoduchý. Představme si abecedu jako nekonečný řádek. Na konci abecedy, po znaku Z bude následovat písmeno A. Každý jednotlivý znak, potažmo písmeno, zaměníme za písmeno posunuté o určitý počet pozic. Za předpokladu, že používáme běžně používanou abecedu, která má 26 znaků máme tedy dohromady 25 různých možností kódování. Při posunutí o 26 znaků by šifrovaný text vypadal stejně jako text vstupní.

Tabulka 1.1: *Příklad Caesarovy šifry s rotací 2 znaky*

Rotace o 2 pozice													
Šifruješ	Y	Z	A	B	C	D	E	F	G	H	I	J	K
Dešifruješ	A	B	C	D	E	F	G	H	I	J	K	L	M
Šifruješ	L	M	N	O	P	Q	R	S	T	U	V	W	X
Dešifruješ	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Příklad: Slovo „Hodiny“ se zašifruje na „JQFKPA“.

Mezi hlavní problém této šifry patří její omezený počet klíčů, tedy počet znaků v abecedě n – 1. Je tedy velmi jednoduchá a s trochou vůle lze vyluštit jen s tužkou a papírem. V dnešní době se používá jen jako příklad klasických šifer a jejich slabin.

- Vzhledem k tomu, že Caesarova šifra má pouze **omezené množství klíčů**, nejjednodušší způsob zlomení šifry spočívá ve **vyzkoušení všech možností** – permutací a zvolit tu, která dává smysl.
- Další možností je frekvenční analýza šifrované zprávy.

Nutno však podotknout, že ve své době tj. na přelomu starého a nového letopočtu měla svůj účel a byla používána pro šifrování vojenských depeší. Patří tedy mezi nejstarší šifrovací algoritmy.

1.4 Moderní šifrovací algoritmy

Hlavní rozdíl mezi klasickými a moderními šifrováním je způsob jejich dešifrování. Zatímco klasické šifry, jako například Caesarova šifra, byly dešifrovatelné pouze s tužkou a papírem, moderní šifrovací způsoby zahrnující složité matematické funkce a k jejich vyřešení je zpravidla třeba velký výpočetní výkon. Na hranici těchto dvou etap lze umístit mechanický stroj Enigma.

1.4.1 Šifrovací stroj Enigma

Enigma[1] byl velmi efektivní německý přístroj používaný převážně během 2. světové války pro šifrování zpráv. Byl podroben mnoha úpravám, nicméně řeč bude převážně o verzi Wehrmacht. Od ostatních verzí se lišila především rozvodnou deskou, která prohazovala jednotlivá písmena klávesnice mezi sebou.

Z čeho se tedy vlastně Enigma, potažmo samotný mechanismus tvořící šifrovaný text, skládal? Prvky budu popisovat ve stejném pořadí, jako funguje šifrovací algoritmus. První část je vstupní klávesnice, velmi podobná klasickému psacímu stroji. Obsahuje celkem 26 písmen včetně klávesy X, která obchází proces šifrování. Další částí je rozvodná deska, jedná se jednoduchou desku s konektory, která dělá pouze to, že navzájem prohodí 2 písmena, tj. např. písmeno G na C a naopak. Třetí je část s rotory. Jedná se o 3 disky, které po každém stisku klávesy otočí. Rotory si lze představit jako hodiny, pomalý, střední a rychlý, kdy rychlý lze považovat za vteřinovou ručičku a pomalý za ručičku hodinovou. Jejich otáčení probíhá tak, že po každém stisku klávesy se otočí rychlý rotor. Jakmile rychlý rotor přejde z hodnoty 26 opět na hodnotu 1, tak se otočí i střední rotor. Stejně tak funguje střední rotor společně s rotorem pomalým. Posledním prvkem Enigmy je samotný zobrazovací systém, který byl zpracován jako jednoduché písmeno podsvícené žárovkou. Enigma jako celek se tedy skládá z vstupní klávesnice, propojovací desky, sady rotorů a sadou žárovek s písmeny. Součástí je samozřejmě také zdroj, ale to je vše, v systému Enigma nebyly žádné procesory řídící šifrování.

1.4.2 Pseudonáhodné číslo aneb proč je tak důležité?

Náhodné číslo v kryptografii je zásadní. Pro šifrování zpráv zpravidla využíváme určitý šifrovací klíč. Tento klíč by teoreticky měl být naprosto nahodilého charakteru. Proč? Jakmile se totiž klíč tvoří podle nějakého vzorce, pravidla, není už příliš těžké odvodit zbytek klíče a tím šifru zlomit.

Pseudonáhodné číslo potažmo jeho generování je proces tvorby sekvence čísel, která se na první pohled zdá být náhodná, avšak není. Pro jejich tvorbu se používají tzv. generátory pseudonáhodných čísel. Ty běží na deterministickém počítači a z principu na nich nelze zcela náhodného čísla dosáhnout.

Pro tvorbu zcela náhodného čísla se v počítačích využívají speciální hardwarové generátory, které generují náhodná čísla na základě ryze fyzikálních veličin. Většinou se jedná o mikroskopické, statisticky náhodné, šumové signály. Dále jsou také využívány zdroje pro určování náhodnosti z oblasti kvantové mechaniky. Jedná se například o radioaktivní rozpad

atomů. Tyto hodnoty jsou v zásadě náhodné. Dalším faktorem podtrhujícím náhodnost je, že každé měření již náhodné hodnoty bude pokaždé jiné z důvodu stále se proměňujících podmínek měření tj. změny teploty, vlhkosti, atmosférického tlaku a dalších interferencí.

1.4.3 Hashování

Jednou z důležitých informací o přijaté zprávě je elektronický otisk. Díky němu má příjemce jistotu, že zpráva nebyla během cesty změněna a zpráva pochází opravdu od odesilatele, který je podepsán. Tedy nejedná se o šifrování samotné, nýbrž o pouhý digitální "otisk prstu".

Hash je jednocestná funkce tj. taková funkce, ze které lze jednoduše zjistit výsledek, ale je velmi obtížně zjistit vstupní data. Tato funkce vytvoří z libovolně dlouhého textu krátký řetězec konstantní délky.

V praxi je hashování využíváno na mnoha místech, např. v hashovacích tabulkách pro usnadnění vyhledávání, v Bloomově filtru pro ověření příslušníků k určité datové množině. Nás ale bude zajímat hashování v bezpečnosti a šifrování.

1.4.3.1 ***Ověření integrity dat***

Integrita znamená, že data jsou správná, celistvá a nezměněná. V praxi se integrita dat prokazuje tak, že na data je použita hashovací funkce společně se sdíleným klíčem. Tato zpráva je poté odeslána příjemci. Ten musí na přijatá data opět použít stejnou hashovací funkci společně s klíčem. Pokud byla zpráva po cestě změněna, a tak narušena její integrita, hash hodnota bude odlišná od hodnoty původní a zpráva tím pádem odmítnuta. Důležité je nakonec říci, že tímto způsobem nelze zaručit pravost dokumentu, tj. od koho data přišla, ale pouze její správnost.

Nevýhodou tohoto systému je, že zpráva může byt odposlechnuta a útočník ji muže poslat znovu popřípadě ji zpozdit a podobně. V případě že by se jednalo o platební příkaz do banky, důsledky by byly nemilé. Příkaz totiž dorazil ve správně formě. Proto existují způsoby jak tomu bránit. Jedna z možností je přidávat do zprávy náhodné číslo tzv. nonce. Tím je každá zpráva unikátní, ale příjemce musí pokaždé kontrolovat, zda mu zpráva s týmž nonce již nepřišla. Pokud ano, zpráva mohla být zneužita.

1.4.4 Symetrické šifrování

Zásadní identifikační znak symetrického šifrovaní[6] je šifrovací klíč, který je stejný jak pro šifrovací proces tak pro dešifrovací. Proto je důležité zajistit bezpečný přenos tohoto klíče. Mezi nejrozšířenější symetrické šifry patří tzv. DES algoritmus, který k šifrování používá 56 bitový klíč. Dnes je však zastaralý. Aktuálně nejbezpečnějším algoritmem je AES, který používá šifrovací klíč délky v rozsahu 128 až 256 bitů.

Výhodou symetrického šifrování je její výpočetní nenáročnost, nevýhodou naopak je, potřeba dešifrovacího klíče k přečtení původní zprávy. Jednou z nevýhod je samotný přenos šifrovacího klíče. Jak bezpečně přenést klíč bez rizika vyzrazeni? Pokud se klíč přenáší elektronickou cestou, je zašifrován pomocí asymetrické šifry, u které není potřeba znalosti klíče. Ten je poté dešifrován u příjemce a následně vložen k dešifrování zprávy.

Druhou nevýhodou je samotná tvorba šifrovacího klíče. Pokud chceme, aby šifra byla dostatečně odolná, je třeba jako šifrovací klíč použít náhodné číslo. V praxi je však generování zcela náhodného čísla přinejmenším obtížné. I ty nejdokonalejší se vyznačují určitou měrou nenáhodnosti. V extrémním případě je pak šifra náchylná k prolomení z důvodu nalezení matematických závislostí v šifrovaném kódu.

Symetrické šifry se dělí na 2 typy. Jedná se o **proudové** a **blokové** šifry. V proudové šifře jsou bity šifrovány jednotlivě, tj. bit po bitu. Naopak u blokových šifer, jsou data rozděleny do bloků o určitém počtu bitů. Délka bloků u šifry AES je 128 bitů.

1.4.5 Asymetrické šifrování

Na rozdíl od symetrického šifrování asymetrické šifrování používá 2 klíče a to jeden tajný – private key a druhý, veřejný – public key. Oba klíče na sobě matematicky závisejí. Zatímco veřejný klíč je určený k zašifrování otevřeného textu popřípadě ověření elektronického podpisu, tak private key slouží naopak k dešifrování šifrovaného textu popřípadě k vytvoření podpisu tj. ověření autora. Zpravidla se při šifrování uveřejní veřejný klíč. Tím je možné zašifrovat jakýkoli otevřený text, ale zpětně dešifrovat lze pouze pomocí privátního klíče, který je znám pouze příjemci. V praxi tak na rozdíl od symetrického šifrování je dešifrovací klíč znám pouze příjemci. Odpadá tak přenos citlivého dešifrovacího klíče skrze otevřený kanál.

Asymetrická funkce podobně jako hashovaní je založeno na jednocestných funkcích. Šifrování pomocí veřejného klíče je zpravidla jednoduché, ale odvození klíče privátního, přestože je matematicky závislý na klíči veřejném, je prakticky nemožné.

1.5 Bezpečnost v bezdrátové telekomunikaci

V následující kapitole přiblížím, jak probíhá komunikace skrze síť GSM – dnešní standard pro telefonií. Bude zde vysvětleno, jak probíhá autentizace účastníka v síti, jaké používá šifrování a proč se nehodí pro přenos šifrovaných informací.

1.5.1 GSM síť

Global System for Mobile Communications (GSM) je aktuálně nejrozšířenější standard pro mobilní telefony po celém světě. Jedná se o druhou generaci systému pro přenos hovorů a signalizace. Dále také podporuje přenos krátkých textových zpráv SMS, datové přenosy a další služby jako je WAP, EDGE, GPRS. Tento standard se vyvíjel od začátku 80. let 20. století a dnes zaujímá více jak 90% trhu. Dle GSMA Intelligence je aktuálně v provozu více 3.5 miliardy unikátních uživatelů a výnosy v tomto odvětví činí 1.13 bilionu dolarů ročně. Ačkoli je tento systém používaný takřka každým v moderní společnosti, GSM zdaleka nepatří mezi bezpečné způsoby komunikace, ačkoli komunikace šifrovaná je. V dnešní době již existují způsoby dešifrování samotného hovoru.

1.5.2 Zabezpečení GSM sítě

Prvním způsobem zajištění bezpečnosti účastníka GSM sítě je autentizace. Autentizace probíhá po každém připojení mobilního telefonu do sítě a zpravidla probíhá tak, že si mobilní telefon a operátor zjednodušeně řečeno vymění autorizační zprávy.

Druhým způsobem zajištění bezpečnosti je šifrování samotného přenosu signálu. Mobilní signál je všude kolem nás a je velmi lehce odchytitelný, takže jediné co uživatele chrání od odposlechu hovoru je právě zvolená forma šifrování. GSM síť používá proudovou šifru, což je symetrická šifra pro kódování prostého textu pomocí pseudonáhodného čísla. GSM využívá několik algoritmů k šifrování komunikace, konkrétně se jedná o algoritmy A5/1, A5/2 a A5/3. Nejsilnější a nejpoužívanější (v Evropě) je algoritmus A5/1, bohužel i tato ochrana je dnes nedostatečná. Bylo zaznamenány mnohé úspěšné pokusy o prolomení této šifry. Ačkoli je GSM protokol pružný a operátor může šifrování zdokonalit, v praxi se tak neděje. Hlavní důvod jsou finance a fakt, že uvádění nových šifrovacích algoritmů do provozu je obtížné. [7]

1.5.3 Prolomení GSM šifrování - algoritmus A5/1

Mezi odborníky ale i běžnými uživateli již dlouho kolují informace o tom, zda šifrovaní GSM pomoci algoritmu A5/1 nebo A5/2 je dostatečné. Jak bylo v minulosti demonstrováno, pomocí různých metod je možné toto šifrování zlomit bez rozsáhlých investic. Existuje několik různých způsobů jak prolomit zabezpečení GSM.

- **IMSI catcher,** jedna z metod, jak proniknout skrze zabezpečení je podvrhnout falešnou BTS stanici. Mobilní stanice po správné realizaci se tak může připojit k této falešné BTS a odchytit tak IMSI.
- **Aktivní odposlech,** tato metoda je založena na funkčním IMSI catcher jednotce. Po připojení mobilní stanice na tuto BTS lze vynutit vypnutí šifrování a odposlouchávat hovor realtime.
- **Pasivní odposlech** je metoda využívající vhodný přijímač signálu, v tomto případě DVB-T tuner, k odchycení samotného hovoru. Následně je daný signál pomoci tzv. Rainbow Tables. Jedná se o přibližně 2TB velký soubor, který umožnuje zpětně dešifrovat zachycenou šifrovanou komunikaci.

Pro podrobné informace odkazuji na diplomovou práci Martina Prokeše z roku 2014[8]. Jsou zde demonstrovány útoky pomocí výše uvedených metod, kdy nejzajímavější se jeví metoda odposlechnutí provozu pomocí DVB-T přijímače. Šifrování GSM tak není dnes vůbec žádná překážka.

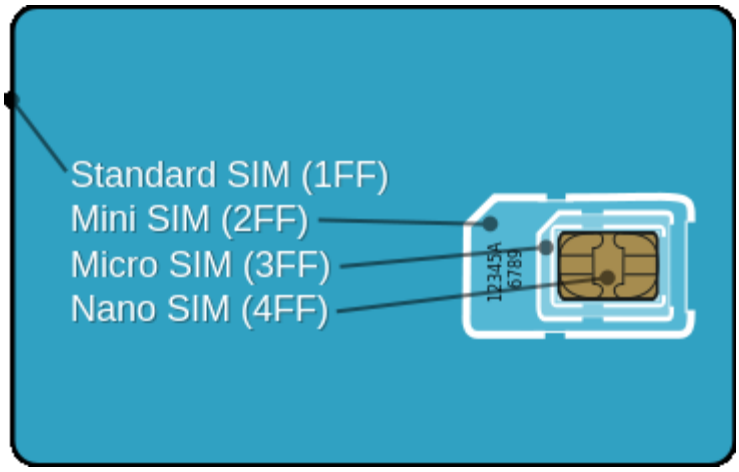
1.6 SIM karta

SIM karta[9] je přenosná čipová karta vybavena mikroprocesorem a paměťovou jednotkou. Obvykle se jedná o osmibitový mikroprocesor ovládaný operačním systémem určeným pro čipové karty. V průběhu let bylo představeno několik různých typů SIM karet, z nichž nejznámější je běžně používaná Mini-SIM. Tyto karty slouží k identifikaci uživatele v

telefonní síti a zaštiťují jak bezpečnost, tak i mnohé funkce, o kterých bude řečeno více v dalších částech studie.

1.6.1 Typy SIM karet

První SIM karta byla vyrobena v roku 1991 v rozměrech klasické platební karty, tj. přibližně 8.5 cm x 5.4 cm. Roku 1996 se na trh dostala SIM karta typu Mini. Tento typ karty aktuálně patří mezi nejpoužívanější, ale pomalu bývá nahrazován v nových mobilních telefonech slotem pro Micro SIM, popřípadě nejnovějším typem Nano SIM, ta byla uvedena na trh v roce 2012.



Obrázek 1.2: Typy SIM karet

Tyto karty jsou navzájem kompatibilní a velikostní rozdíly se řeší pouze na hardwarové úrovni, tj. jednoduše použitím vymezovacích adapterů. Běžně se také z klasické Mini-SIM karty přechází na Micro SIM nebo Nano SIM verze pouhým použitím nůžek či ostrého nože.

S novými rozměry získávaly SIM-karty také na nových funkcích a samotných prostředcích. Zatím co první SIM karty, tj. fáze 1., nepodporovaly ukládání SMS zpráv ani telefonních kontaktů a měly paměť pouhých 8 kilobytů, dnešní karty, fáze 2+, běžně poskytují až 128 kilobytů paměti. Výjimkou nejsou ani speciální SIM karty s velikosti dosahující 1 gigabytu, tyto karty však nejsou běžně používány.

1.6.2 Autentizace SIM karty v GSM síti

Název SIM karty je odvozen od prvních písmen anglického názvu Subscriber Identification Module. Hlavní funkce SIM karty je tedy bezpečná identifikace účastníka v mobilní síti a k tomu využívá několik důležitých čísel.

První z čísel je ICCID, jedná se o výrobní číslo SIM karty. Používá se pouze k administrativním účelům a lze ho přečíst na zadní části karty. Číslo se skládá z několika částí. První část obsahuje IIN číslo SIM karty. Skládá se z ID operátora, státu a účastníka. Druhá část obsahuje individuální číslo různé délky, avšak má stejnou délku jako IIN. Posledním číslem je

check digit, což je samostatné číslo generované pomocí Luhnova algoritmu. V praxi jsou ICCID 19 nebo 20 místná unikátní čísla.

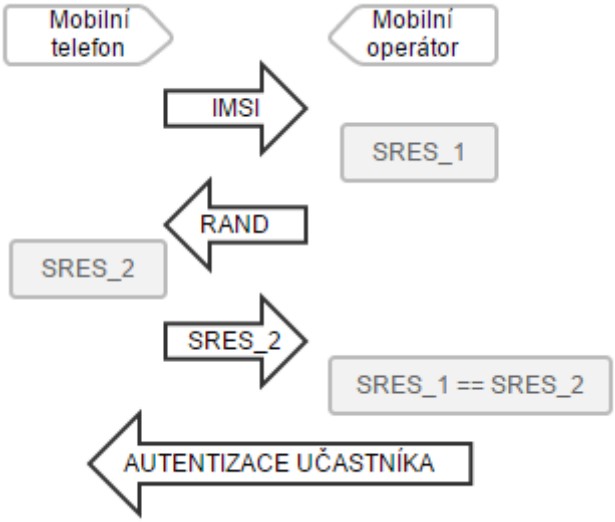
Dalším důležitým číslem je IMSI, což je mezinárodní identifikační číslo, na rozdíl od všech následujících je veřejné. IMSI slouží jako spojovací číslo do databáze mobilního operátora. Až v té je totiž uložené účastnické číslo, tj. číslo, které "voláme".

Tyto dvě čísla tedy označují různá identifikační čísla účastníka v síti, nicméně nemají nic společného se samotnou komunikací, autorizací. Pro tuto část je důležitý autentizační klíč Ki.

Klíč Ki je 128 bitové unikátní číslo přidělené operátorem při uvedení karty do provozu. Tak jako IMSI, je ověřovací klíč Ki uložen v databázi mobilního operátora. Obecně je SIM karta navržena tak, aby nefungovala, pokud její data nejsou podepsány právě tímto klíčem. Nicméně i tak zde jsou způsoby, jak klíč ze SIM karty extrahovat, vytvořit duplikát.

Jak tedy vlastně funguje samotný princip autentizace[9][10] účastníka?

1. Po zapnutí mobilního telefonu si SIM karta může vyžádat PIN kód. Po jeho potvrzení je operátorovi odeslán požadavek o přístup do sítě. Ten obsahuje právě IMSI, identifikační číslo SIM karty.
2. Operátor si IMSI vyhledá v databázi. Následně k němu přiřadí ověřovací klíč Ki, který je rovněž uložen v databázi již od uvedení SIM karty operátorem do provozu.
3. Operátor dále vytvoří unikátní náhodné číslo RAND a to podepíše klíčem Ki. Vzniká tak zpráva tzv. Signed Response 1 - SRES_1. Tato zpráva zůstává v operátorově databázi a čeká.
4. Stejné náhodné číslo RAND, jako v minulém kroku, je odesláno do mobilního zařízení a je předáno SIM kartě. Karta následně číslo RAND zašifruje šifrovacím klíčem Ki pomocí A38 algoritmu. Vzniká tak zpráva tzv. Signed Response 2 - SRES_2. Tato zpráva je následně odeslána zpět operátorovi. Vzniká také šifrovací klíč Kc, který zůstává v mobilním telefonu. Telefon podle tohoto klíče šifruje A5/1 algoritmem všechnu další komunikaci mezi mobilním telefonem a základnovou stanicí - BTS. Algoritmus A5/1 je součástí mobilního telefonu, na rozdíl od A38 algoritmu, který je integrován v SIM kartě.
5. Operátor následně srovnává SRES_1, uloženou v databázi, s SRES_2, přijatou od mobilního telefonu. Pokud se hodnoty shodují, autentizace mobilního telefonu je úspěšná.



Obrázek 1.3: Zjednodušený model autorizace účastníka mobilní sítě

1.6.3 SIM karta a soukromí uživatele

Každá SIM karta[9][10] ukládá plno informací o uživateli, které průběžně odesílá zpátky operátorovi a ten následně tyto údaje může jak legální tak ilegální cestou poslat dále. Mezi nejdůležitější data patří informace o volaných a obdržených telefonátech. V České Republice je zákonem daná lhůta 6 měsíců, která ukládá operátorovi tyto záznamy archivovat.

Dalším důležitým údajem, který je zasílán operátorovi je LAI, což je informace o umístění SIM karty na mapě. Operátor má svoji oblast působení rozdělenou na různě velké segmenty a každý ze segmentů má vlastní identifikační číslo. Toto číslo je uloženo v SIM kartě a je využíváno k tomu, aby SIM karta při zapnutí mobilního telefonu nemusela pokaždé prohledávat všechny možné frekvence pro nalezení signálu. Stačí, aby dle aktuální pozice vyhledala příslušného lokálního poskytovatele. SIM karta nicméně ukládá LAI do seznamu při každé změně umístění. Zpětně tak lze jednoduše vystopovat, kde a kdy SIM karta byla, popřípadě aktuálně je.

2 Současné možnosti šifrování mobilních telefonů

Jak již bylo řečeno v minulé kapitole, GSM komunikace již není dostatečně bezpečná k přenosu citlivých informací. Proto se vývojáři rozhodli tento způsob spojení obejít. K přenosu dat tak využívají nikoli GSM, ale datové přenosy – internet. Ten poskytuje vyšší přenosové rychlosti, ale především umožnuje vlastní formu šifrování dat a není vázán na šifrovací standard GSM – šifru A5/1. Pro přenos hlasu využívají tzv. VoIP neboli Voice over Internet Protocol. Jedná se o přenos hlasu skrze internet.

2.1 SIP protokol

Všechny následující aplikace využívají SIP protokol[11] nebo velmi podobnou alternativu. Jedná se o internetový protokol určený k přenosu signalizace v internetové telefonii. Většinou funguje formou UDP datagramu, ale je ho možné přenášet i pomoci TCP. Tento protokol má na starost samotné navázání a udržování spojení.

Činnosti protokolu

- Lokalizace účastníka
- Zjištění stavu účastníka
- Zjištění možností účastníka
- Vlastní navázání spojení
- Řízení probíhajícího spojení

Chybová hlášení

- 1xx - průběh
- 2xx - úspěch
- 3xx - přesměrování
- 4xx - chyba klienta
- 5xx - chyba serveru
- 6xx - fatální chyba

Metody protokolu

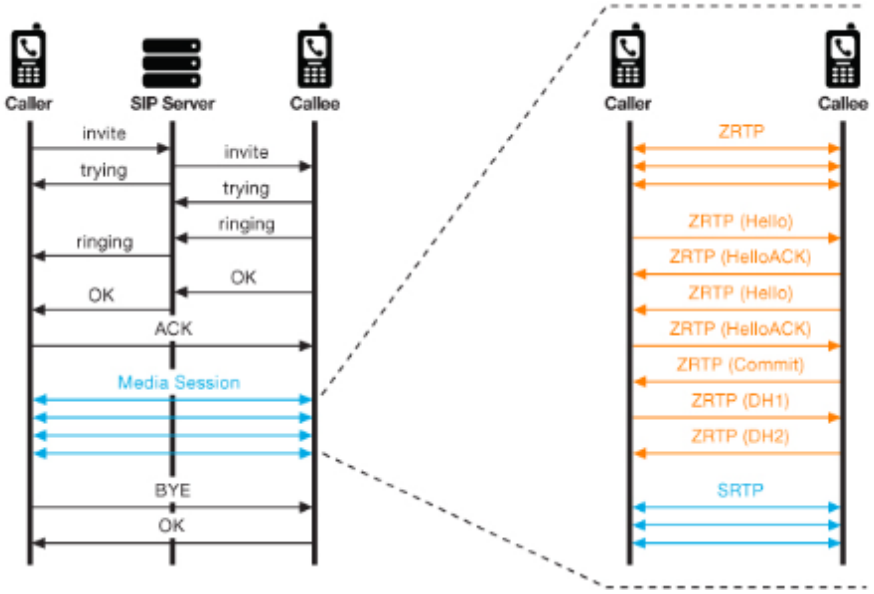
- REGISTER - registrace účastníka na SIP Proxy serveru
- INVITE – zahájení komunikace o plánované nové relaci
- ACK – potvrzení zahájení relace
- CANCEL – přerušení zahajovaní relace ještě před jejím navázáním
- BYE – ukončení relace
- OPTIONS – požádá o informace o možnostech volajícího, aniž by se sestavilo volání

2.2 ZRTP protokol

ZRTP[12] je kryptografický key-agreement protokol, který umožnuje dvěma a více stranám dohodnout se na společném šifrovacím klíči, za společné účasti na jeho podobě, v online telefonních hovorech založené na VoIP protokolu.

ZRTP je založen na RTP protokolu. Ten využívá D-H algoritmus a SRTP protokol pro samotné šifrování. Jedná se tedy o protokol k výměně klíčů, při hovoru navázaném v reálném čase pomocí jiného protokolu, jako je např. SIP v tomto případě. Tím se vytvoří tajný sdílený klíč, který se používá pro vytváření dalších klíčů potřebných při komunikaci pomocí SRTP protokolu. Klíč je generován při každém vytvoření relace tj. komunikačního spojení. Samotné „Z“ ve zkratce značí jeho hlavního tvůrce Phila Zimmermanna. Tento protokol byl publikován v roce 2011 jako RFC 6189[13].

ZRTP lze přenášet pomocí jakékoli telefonní síti včetně GSM, UMTS.



Obrazek 2.1: Funkce SIP a ZRTP

2.3 Placené šifrovací řešení a služby

Další možností zabezpečení je pořízení speciálních mobilních telefonů s vlastními způsoby zabezpečení. Zpravidla je zabezpečení na „vojenské úrovni“, avšak to je vykoupeno cenou, která může být příznivá pouze pro uživatele disponujícími velmi diskrétními informacemi, a jsou ochotni zaplatit vysoké částky pro jejich uchování v tajnosti.

Jako příklad zvolím produkty od firmy Probin.cz. Poskytuje zabezpečovací služby, jak co se týče šifrování tak i realizace odposlechů a vyhledávání štěnic. My se zaměříme pouze na jejich služby v oblasti zabezpečení telefonní komunikace.

2.3.1 **Probin – šifrovací mobilní telefony**

Firma Probin[14] poskytuje své šifrovací mobilní telefony vybavené zabezpečovací technologii CryptoSmart. Svým zákazníkům nabízí 2 typy mobilních telefonů vybavené CryptoSmart kartou. Nejdřív tedy rozeberme ji. Jedná se o běžnou MicroSD flash paměť obsahující mikroprocesor pro hardwarový generátor náhodných čísel. Následuje výčet „schopností“ CryptoSmart karty. Bohužel z tohoto popisu nelze příliš zjistit.

- Hardwarový generátor náhodných čísel
- Výpočet nového šifrovacího klíče před každým voláním nebo přenosem dat
- Správa klíčů
- Spolehlivé šifrování založené na RSA algoritmu
- Soukromý klíč integrovaný ve smart kartě není možno obnovit ani “hrubou silou”
- Autentizace uživatele pomocí 4 až 8 místného PIN kódu
- Autentizace volajícího
- Výměna klíčů mezi kartami - klíč není nikdy přímo použit žádnou externí aplikací
- Vzdálené odblokování Cryptosmart karty pomocí jednorázového 8 místného PUK kódu
- Správa karty se provádí připojením karty do USB nebo kartové čtečky, která je připojena na Cryptosmart CardManager – PC.
- Komunikovat mohou mezi sebou pouze terminály obsahující karty pocházející ze stejné “rodiny”

Po přečtení bodů bych možnosti karty shrnul takto. Hardwarový generátor náhodných čísel je jistě zásadní plus tohoto modulu. Naopak výpočet nového klíče je nutný předpoklad kvalitního šifrování a jedná se, jako další řádky, především o marketingovou „omáčku“ aby byl zákazník „povolnější“.

Nyní se podívejme na samotné mobilní telefony nabízené danou firmou. Nabízí mobilní telefon S:Phone a modifikovaný Samsung Galaxy S3 CryptoSmart.

S:Phone je mobilní telefon vybaven vlastním operačním systémem speciálně navržený pro komunikaci v CryptoSmart síti. Jak lze poznat dle obrázku, ale i specifikací na webových stránkách patří tento přístroj do nejnižší cenové kategorie. Na druhou stranu priorita je bezpečnost. Podívejme se na druhý poskytovaný mobil.

Obrázek 2.2: S:Phone

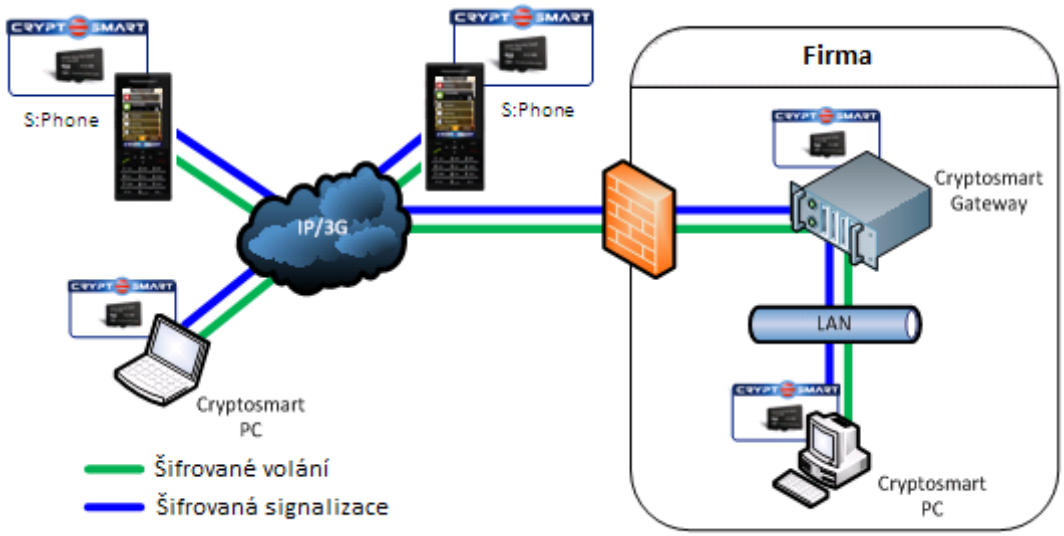
Obrázek 2.3: Samsung Galaxy D3

Druhý nabízený přistroj je Samsung Galaxy S3 CryptoSmart. I tento mobilní přístroj již není nejnovější nicméně na rozdíl od S:Phone patří alespoň do kategorie smartphone a tak poskytuje určité pohodlí, na které jsou dnešní uživatelé zvyklí. Oba přístroje se pyšní následující šifrováním.

- Hardwarový klíč zabezpečující šifrování
- Certifikováno EAL4+ (nejvyšší možná úroveň certifikace systému pro komerční využití)
- Autentizace vzdálené karty (RSA 2048 bitů)
- Šifrování hlasové komunikace (AES 256 bitů)
- Šifrování SMS (AES 256 bitů)
- Šifrování osobních dat – SMS, kontakty, výpisy volání, soubory, fotky (AES 256 bitů)
- Poskytnutí zabezpečeného serveru (Gateway)
- Uživatelská podpora 5 dní v týdnu 9:00 - 17:00.

Jak jde vidět, šifrování je více jak dostatečné a výrobce opravdu poskytuje šifrované mobilní telefony, které jsou poskytnout vysokou úroveň zabezpečení. Nyní se podívejme jak vlastně CryptoSmart systém funguje.

2.3.2 CryptoSmart síť



Obrázek 2.4: Šifrované volání a signalizace

CryptoSmart systém je založen na VoIP komunikaci, veškeré přenosy hlasu jsou tak posílány skrze datové sítě. Síť poskytuje šifrovaný provoz pro všechny uživatele ve stejné síti. Tzn. pouze pro uživatele CS sítě. Zároveň ale umožnuje spojení i mezi normálními účastníky sítě GSM, avšak již bez šifrování.

Důležité na konci tohoto krátkého bloku je celkově shrnout placené služby tohoto poskytovatele a samozřejmě také kolik tyto služby stojí.

CS systém poskytuje nadprůměrné možnosti šifrování a věřím, že tento systém může být velmi užitečný. Data nejsou přenášeny skrze zranitelnou GSM síť nýbrž skrze bránu (server) CS systému. Komunikace je tak realizována ve vlastní soukromé síti. Problém je, že pokud volaný nedisponuje stejným systémem, šifrovaní je pryč. Nyní k ceně.

Cena mobilního telefonu Samsung Galaxy S3 je 85 000kč. To je částka, za kterou získáte mobilní telefon a 3 letou možnost telefonování v privátní síti. Dovolím si soudit, že tato cenovka odradí 99% zákazníků. Pro zbylé 1% cena není prioritní a neví o alternativách.

2.4 Open source řešení zdarma a pro každého

Důležité je říci, že se mi nepodařilo najít jakýkoli způsob jak šifrovat telefonní hovory skrze GSM samotnou. Veškeré níže uvedené aplikace proto používají k šifrování datové přenosy. V některých případech je možné se dovolat z šifrovací aplikace skrze datové přenosy na mobilní telefon připojený pouze k GSM síti, toto je však umožňováno pouze za poplatek. Bezplatný a šifrovaný provoz je tedy zpravidla umožněn uživatelům připojeným k internetu a využívající aplikaci pro daný šifrovací nástroj.

V následujících kapitolách představím několik nejzajímavějších aplikací umožňujících utajení většiny dnešního běžného provozu. Bude se jednat jak o telefonní hovory z mobilu na mobil tak i na stolní počítače či tablety. Budou také představeny aplikace pro šifrování SMS zpráv, bezpečné prohlížení internetu či IM klient s rozsáhlou podporou protokolu a jejich šifrování.

RedPhone

https://whispersystems.org/
Funkce: šifrování telefonních hovorů
Platforma: Android
Cena: Zdarma; open source

Ostel

https://ostel.co/faq
Funkce: šifrování telefonních hovorů
Platforma: And, iOS, Mac, Windows, Linux, BlackBerry
Cena: zdarma; pro iOS za poplatek

Silent Phone

https://www.silentcircle.com/
Funkce: šifrování telefonních hovorů
Platforma: Android, Windows Phone
Cena: začíná na 12.95$ měsíčně

Chat Secure

https://guardianproject.info/apps/chatsecure
Funkce: šifrovaný IM klient.
Platforma: Android, iOS, Mac, Linux, Windows
Cena: Zdarma

Orweb

https://guardianproject.info/apps/orweb
Funkce: skrytí identity skrze TOR síť.
Platforma: Android
Cena: Zdarma

Orbot

https://guardianproject.info/apps/orbot/
Funkce: skrytí IP adresy
Platforma: Android, iOS
Cena: Zdarma

2.5 The Guardian Project

Skupina TGP[15] se věnuje vývoji různých bezpečnostních aplikací. TGP je sdružení technologických nadšenců, vývojářů zabývající se tvorbou dostupných nástrojů na základě dnešních požadavků na bezpečnost.

Konkrétně se TGP zabývá tvorbou open source knihoven a aplikací pro mobilní telefony na nich stojících. Veškerá jejich tvorba patří do kategorie open source, tím pádem jsou veřejně dostupné zdrojové kódy. Ty poté mohou využity k vývoji vlastních aplikací, ale také jsou podrobovány kritickému oku veřejnosti. Tím je zaručeno, že kódy neobsahují žádné skryté zadní vrátka.

Jednou z hlavních výhod aplikací od TGP je jejich multiplatformnost. Jejich aplikace, ve většině případů, podporují všechny rozšířené platformy. Mezi podporované platformy patří Android, iOS a Mac, Windows, Linux a BlackBerry.

Díky aplikacím od TGP tak máme možnost volat mezi mobilními telefony různých operačních systémů v šifrované podobě. Můžeme posílat šifrované zprávy, ale i procházet webové stránky pomocí bezpečného prohlížeče přistupujícího k internetu pomocí sítě Tor.

Hlavním tématem této práce však bude šifrovaný telefonní hovor a TGP poskytuje jednu z aplikací, kterou budu testovat. Jedná se o řešení Ostel – šifrovaný VoIP server. Přestože se tato práce má soustředit především na hovory, velmi lehce se také dotknu ostatních aplikací, které mohou také velkou měrou zvýšit bezpečnost uživatele v Internetu.

2.5.1 ChatSecure: Private Messaging

ChatSecure[20] potažmo TextSecure je bezplatná open source aplikace s možností OTR šifrování pomoci XMPP protokolu. Díky tomu aplikace umožnuje se připojit k většině současně používaných IM aplikací jako je Facebook XMPP, Google Talk a podobně. Aplikace je dostupná jak pro Android, tak i pro iOS.

OTR je kryptografický protokol poskytující šifrování pro IM komunikátory. OTR používá kombinaci několika šifrovacích algoritmů. Jedná se o 128 bitový AES šifrovací algoritmus, dále D – H algoritmus, který se stará o přenos šifrovacího klíče skrze veřejně dostupný kanál a hashovaní pomocí SHA-1.

2.5.2 Orbot: Mobile Anonymity + Circumvention

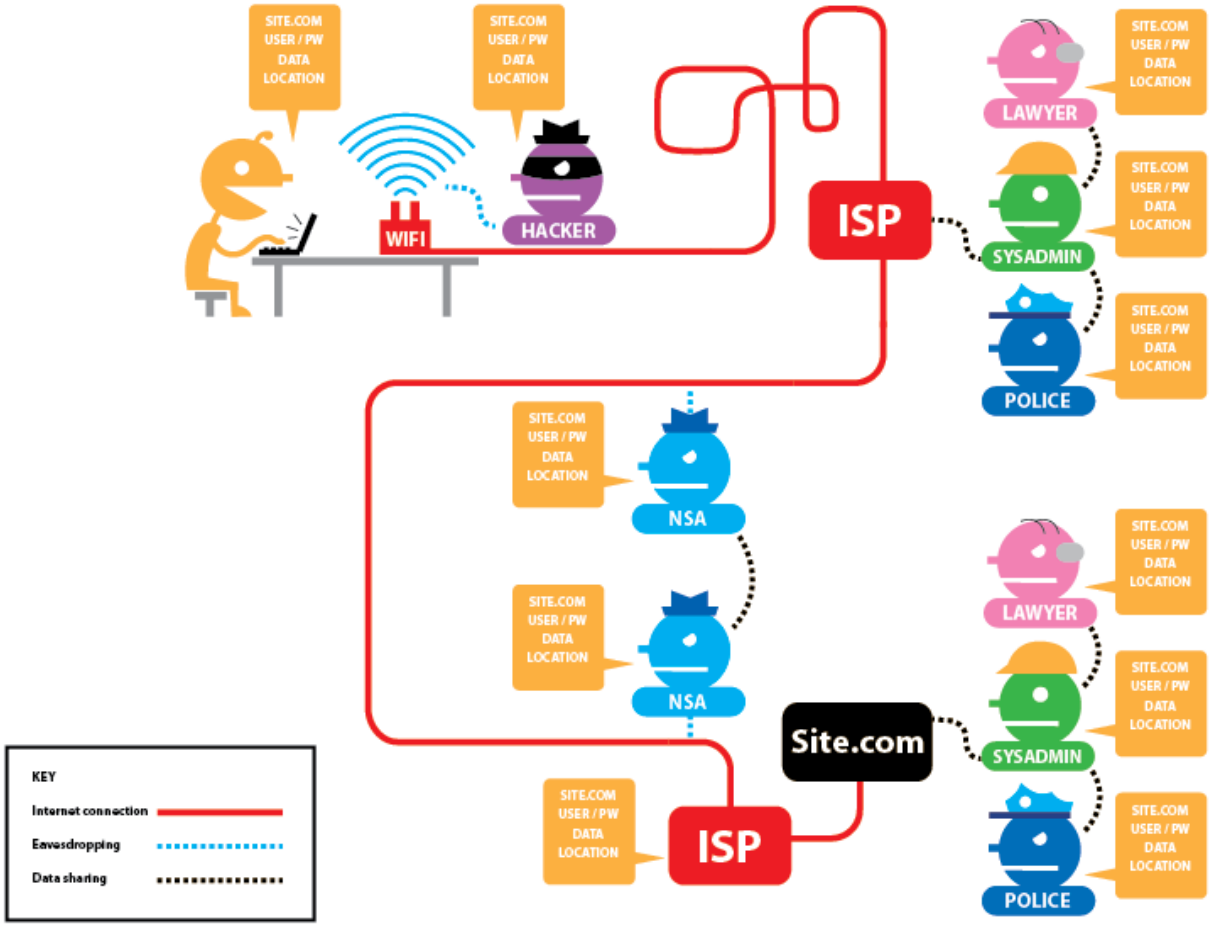
Orbot[18] je aplikace umožňující mobilnímu telefonu skrýt identitu. Využívá k tomu síť Tor. Jedná se o velmi jednoduchou, uživatelsky přívětivou aplikaci, ve které stačí pouze nastavit provoz jaké aplikace má být skryt. Každá aplikace zahrnutá v nastavení Orbot bude v internetu vystupovat pod novou IP adresou. Díky této aplikaci tak lze zásadně znesnadnit potencionálnímu útočníkovy jakoukoli snahu o získání informací o činnosti na Internetu.

2.5.2.1 Jak funguje síť Tor?

Princip fungovaní sítě Tor je jednoduchá. Každý účastník sítě Tor se automaticky stává šifrovacím prvkem sítě. Komunikace probíhá tak, že se vytvoří šifrované spojení mezi účastníkem

a cílem. Mezi tyto 2 cíle je však vloženo n různých mezi uzlů s tím, že každý z uzlů zná pouze předchozí uzel – odesílatele a následující uzel – příjemce. Již při malém počtu mezi uzlů se tak stává zpětné hledání odesilatele zprávy velmi obtížná.

Ukažme si modelový příklad, účastník U chce kontaktovat server S, čili např. běžné prohlížení Internetu pomocí HTTP. V prvním kroku si U vyžádá od serveru TORu seznam dostupných uzlů. Ten poté U pomocí aplikace vytvoří bezpečnou trasu skrze Internet až k příjemci. Na této trase probíhá veškerá komunikace fungující na TCP protokolu. Jiný protokol není podporován. Každý takto vytvořený šifrovaný okruh trvá asi 10 minut. Poté je proces zopakován a je vytvořena zcela nová cesta. Tím se uživatel stává „novým“ účastníkem a veškerá jeho předchozí činnost je „ztracena“.



Obrázek 2.5: Proč skrývat aktivitu na síti pomoci Tor sítě

2.5.3 Orweb: Private Web Browser

Jak název napovídá, jedná se o anonymní webový prohlížeč[16]. Využívá výhody Tor sítě čerpající z aplikace Orbot[18] a přidává mnoho dalších možností jak skrýt veškerý provoz před ostatními účastníky internetu.

Hlavní výhody oproti běžným webovým prohlížečům:

- **Žádná historie prohlížení**
- **Kontrola Cookies** umožnuje jednotlivým serverům, povolit či zakázat ukládání cookies. Ty jsou ukládány v prohlížeči a při další návštěvě serveru jsou opět odeslány na server a informují jej o předchozí činnosti uživatele. V cookies jsou např. uloženy navštívené stránky, ale i informace o přihlášení uživatele tj. heslo. Při získání cookies lze pak informace zneužít třetí stranou.
- **Zamaskuje IP adresu** pomocí Tor sítě.
- **Defaultně blokuje JavaScript** čímž zabrání velmi časté formě útoku. JavaScript samozřejmě lze spustit tam, kde si jsme jisti obsahem.
- **Ošetřuje bezpečnostní chyby Flash aplikací**, které mohou zneužity k útoku.

Mezi další výhody patří také rozsáhlá jazyková podpora. Aplikace je také často aktualizována. Orweb je momentálně dostupný pouze pro Android. Jeho verze pro iOS je ve vývoji. Alternativou pro iOS je tak Onion Browser s velmi podobnými funkcemi.

Orweb je skvělá možnost pro internetové uživatele, kteří ocení naprostou kontrolu nad daty, které odesílají do internetu a cení si svého soukromí nadevše. S využíváním této úrovně zabezpečení však přicházejí také ústupky na straně uživatele a určitá ztráta pohodlí. Webové stránky spíše nefungují, dokud je vypnut JavaScript. Některé servery nemusí být dostupné pro přidělenou IP adresu z důvodu blokace. S vypnutou historii prohlížení nebude nikdy „napovězen“ oblíbený web. Prohlížeč si také nebude pamatovat přihlašovací údaje. Volba je na každém z nás.

2.5.4 Ostel – Encrypted phone calls

Ostel je open source šifrovací nástroj pro poskytování end-to-end šifrovaných telefonních hovorů. Ostel poskytuje bezplatné možnosti hovorů mezi většinou používaných operačních systému. Příslušnou aplikaci odpovídající operačnímu systému podporující Ostel popisuje následující tabulka. Veškeré aplikace níže zmíněné jsou spolu navzájem kompatibilní.

Tabulka 2.1: *Podpora Ostel na různých platformách*

Platforma	Android	iPhone	BlackBerry	Mac	Windows	Linux
Aplikace	CSipSimple	Acrobits Softphone	PrivateGSM	Jitsi	Jitsi	Jitsi

Velkou nevýhodou tohoto systému, kde každá platforma využívá jinou aplikaci, je pocit necelistvosti. Produkt nevypadá dostatečně profesionálně, jak by se od aplikace na bezpečnost komunikace očekávalo. Je to dáno tím, že každou aplikaci vyvíjel někdo jiný a podpora sítě Ostel.co bylo přidáno jen jako podpora dalšího z mnoha VoIP serverů.

Ostel je postaven na dvou hlavních technologiích a to na SIP protokolu a Ruby on Rails. SIP server s názvem Kamailio zaštiťuje úvodní signalizaci a udržuje spojení. Veškerý provoz skrze Ostel je veden skrze internet a pro provoz je zásadní vlastnit dostatečný datový tarif pro správný provoz aplikace. End-to-end šifrování je zprostředkováno skrze ZRTP protokol.

2.6 RedPhone

RedPhone[19] je druhá open source aplikace, která bude součástí testování. Jedná se o aplikaci od Open Whisper Systems. Podporuje pouze prostředí Android. Funguje na stejném principu jako konkurenční Ostel. Komunikace je šifrována pomoci SRTP protokolu, přenos a vytvoření samotného klíče je v režii protokolu ZRTP. Samotná již šifrovaná data jsou ještě přenášena pomocí TLS.

3 Výběr aplikací a testování

V této kapitole se pokusím pomocí výše zmíněných aplikací navrhnout ideální softwarové vybavení moderního mobilního telefonu s operačním systémem Android OS. Dále se pokusím odchytnout provoz mezi volajícím/odesílatelem a příjemcem telefonátu, potažmo zprávy. K tomu využiji programy Wireshark, 4G Mark, G-NetMark. K testování použiju své vlastní vybavení.

Vybavení k uskutečnění a následné analyzování provozu je následující hardware:

Mobilní telefon LANDVO L200G

Rozměry: 72 x 144 x 8.6 mm
Váha: 153g
CPU: ARM Cortex-A7, 1300MHz, počet jader: 4
GPU: ARM Mali-400 MP2, 416MHz, počet jader: 2
RAM: 1GB, 533 MHz
OS: Android 4.4.2 KitKat
WIFI: b, g, n

SIM karty
Poskytovatel: T-Mobile
Technologie: 4G LTE, 3G

Notebook LENOVO Y550P

CPU: Intel Core i3, 2.27GHz
GPU: nVidia GeForce GT 240M
RAM: 4GB, 800MHz
OS: Windows 8.1 Pro
WIFI: b, g, n
Diagnostické aplikace: Wireshark

Mobilní telefon Sony Xperia M

Rozměry: 124 x 62 x 9.3 mm
Váha: 115 g
CPU: Dual-core 1 GHz Krait
GPU: Adreno 305
RAM: 1 GB RAM
OS: Android 4.1 Jelly Bean
WIFI: b, g, n
Diagnostické aplikace: Intercepter-NG
HSPA: podporováno
LTE: nepodporováno

3.1 4G internet od T-Mobile

Pro uskutečnění pokusů jsem si zajistil SIM karty z Katedry telekomunikační techniky. Jedná se o 2 SIM karty značky T-Mobile vybavené datovým tarifem. T-Mobile nabízí pokrytí LTE a 3G technologii. Měření rychlosti této sítě jsem uskutečnil pomocí mobilu Sony Xperia M. Protože se nejedná o nejnovější mobilní telefon, podpora LTE zde není zajištěna. Datové přenosy tak byly realizovány skrze technologie HSPA+.

Tabulka 3.1: *Naměřené hodnoty T-Mobile – parametry připojení*

Typ	Technologie	Rychlost [Mbps]	Doba odezvy [ms]
Downlink	3G - HSPA+	5.08	///
Uplink	3G - HSPA+	1.49	///
RTT	3G - HSPA	///	299

Vzhledem k tomu že mobilní telefon nepodporuje nové LTE, nelze soudit, jaká by byla reálná rychlost internetu, kterou operátor avizuje a kterou doopravdy poskytuje. Pro testování aplikace je připojení dostačující. Hodnoty byly naměřeny pomocí aplikace 4Gmark pro testování rychlostí datových sítí.

3.2 Domácí WIFI připojení

Jak lze z porovnání hodnot usoudit, zavedené WIFI na vesnici je na dnešní dobu velmi pomalé a je na podobné úrovni jako spojení skrze mobilní datové sítě, která je navíc omezena možnostmi mobilního telefonu. Zásadní rozdíl je však v rychlosti odezvy.

Tabulka 3.2: *Naměřené hodnoty WIFI – parametry připojení*

Naměřené hodnoty WIFI – parametry připojení			
Typ	Technologie	Rychlost [Mbps]	Doba odezvy [ms]
Downlink	WIFI	5.48	///
Uplink	WIFI	1.74	///
RTT	WIFI	///	21.81

3.3 Kvalita hovoru

Pro určení kvality hovoru budu používat subjektivní metodu měření kvality hovoru. Ta se bude řídit běžnou stupnici MOS. Subjektivní metodu volím zvláště pro obtížné zachycení všech důležitých vstupních dat pro objektivní metody. Všechna měření probíhala v tichém, ničím nerušeném prostředí.

Tabulka 3.3: *Hodnoty stupnice MOS*

MOS	Kvalita	Popis
5	Vynikající	Neznatelné rušení
4	Dobrá	Rušení lze rozpoznat, ale není obtěžující
3	Průměrná	Rušení lze rozpoznat a mírně obtěžuje.
2	Nízká	Rušení obtěžuje, je nutno vyvinout úsilí při snaze porozumět.
1	Špatná	Rušení velmi obtěžuje, řeč je nesrozumitelná.

3.4 Způsob měření

Měření budou probíhat na 2 platformách a to spojení mobilní telefon – mobilní telefon. Druhé měření bude mezi mobilním telefonem a notebookem. Obě měření budou probíhat na 2 různých připojení k internetu. Využiji připojení pomocí datové sítě od T-Mobile. Druhou volbou je domácí WIFI připojení.

3.5 Výběr a spuštění zvolených aplikací

Jako další krok je volba vhodných aplikací k šifrování. Vzhledem k tomu, že výběr aplikací je omezen na freeware řešení pro platformu Android. V předešlé kapitole byly představeny aplikace od The Guardian Project a jeho Ostel, dále také RedPhone od Open Whisper Systems.

3.6 Příprava na měření a seznámení s aplikacemi

3.6.1 Ostel

Pro šifrování samotného telefonního hovoru využijeme Ostel – první ze dvou testovaných aplikací pro VoIP. Na mobilní telefon nainstalujeme aplikaci CSipSimple. Jedná se o aplikaci podporující připojení právě k VoIP serveru Ostel.co, který zaštiťuje komunikaci mezi 2 koncovými stanicemi. Tuto aplikaci budu považovat za výchozí při hodnocení pro platformu Android.

Tuto aplikaci stáhneme v Google Store. Po instalaci je třeba přidat účet, který se již vytvořil na domovské stránce Ostel.com. Po přidání účtu se aplikace automaticky připojí a mobil je připraven uskutečňovat telefonní hovory a posílat zprávy.

Pro testovací účely vytvoříme 2. účet na stránkách Ostel.com. Ten následně využijeme pro zprovoznění druhé stanice.

Druhou stanicí bude notebook vybavený aplikací Jitsi. Jitsi je open source aplikace pro internetovou telefonii a instant messenger, který podporuje mnoho komunikačních protokolů jako je SIP, ale i XMPP (možnost připojení k Facebook chat, či Google Talk).

Zajímavostí při tvorbě účtu na Ostel.co je, že účty zde nejdou zrušit. Na první pohled se tento fakt může jevit jako bezpečností riziko. Na druhou stranu, tvorba účtu nevyžaduje žádné osobní data mimo e-mailu. Výčet všech požadavků k tvorbě účtu tak je pouze e-mail, heslo a přezdívku. Při použití bezpečného e-mailu, který je nespojitelný s osobou používající Ostel tak není možnost jak přiřadit komunikaci konkrétnímu uživateli.

Bezpečný e-mail je zpravidla takový, který není na internetu známy, není přiřazený k různým službám a při jeho tvorbě nebyly použity žádná osobní data.

Identifikace účastníka

- SIP URI: login@ostel.co

Klady

- Zdarma
- Možnosti nastavení
  - Nahrávání hovoru
  - Volba kodeků
  - Podpora stovek VoIP poskytovatelů
- Kvalitní zabezpečení¨
- Podpora „SMS“

Zápory

- Nedostatečná integrace do systému
- Nedokonalé grafické prostředí
- Složitější instalace a konfigurace

Ostel nabízí kvalitní bezplatné řešení jak komunikovat skrze šifrovaný kanál. Relativně komfortně, s bohatými možnostmi nastavení. Taktéž možnost posílání zpráv usnadňuje mnohé.

3.6.2 **RedPhone**

Druhá testovaná aplikace pro VoIP je RedPhone[19]. Jedná se o open source aplikaci vyvíjen pro Android od Open Whisper Systems. Stejně jako Ostel využívá k šifrování ZRTP protokol. Síť je složena z 2 typů serverů[25]. Jedná se o servery Master a Relay. Master servery se starají o počáteční signalizaci a autentizaci. Jsou umístěny na důvěryhodných místech s omezeným přístupem. Naopak servery typu Relay jsou rozmístěny různě po planetě, aby zajišťovaly uživatelům co nejnižší odezvu. Tyto servery se starají o samotné udržování již navázaného, ověřeného spojení.

Aplikace se stahuje z Google Store jak jsme zvyklí. Po instalaci je nastavení omezeno na pouhé přiřazení běžného telefonního čísla k právě nainstalované aplikaci RedPhone. Telefonní číslo je přiřazeno anonymnímu účtu na serveru a to je jediný identifikační údaj aplikace. S každou novou instalací aplikace se tak telefonní číslo přiřazuje novému anonymnímu účtu. Tím končí veškeré nastavení.

Manipulace s aplikací je o poznání jednodušší a grafické rozhraní přehlednější než u předchozího produktu. Velmi dobře byl vymyšlen systém identifikace uživatele a přidávání kontaktů. Při spuštění aplikace se synchronizuje telefonní seznam mobilního telefonu s databází RedPhone serveru. Pokud najde shodu, tzn., najde v telefonním seznamu uživatele RedPhone aplikace, vloží ho do svého vlastního seznamu. Vše se tak děje automaticky. Na rozdíl od řešení Ostel, který používal k identifikaci SIP URI formát, RedPhone používá telefonní číslo, které stačí uložit jako běžný telefonní kontakt.

Identifikace účastníka

- Původní telefonní číslo

Klady

- Jednoduchost
- Anonymita
- Rychlost instalace
- Kvalitní grafické rozhraní
- Integrace

Zápory

- Absence jakéhokoli nastavení
- Neprůhlednost systému

Aplikace RedPhone je z mého pohledu dokonalá. Působí profesionálním dojmem, zaměřením se pouze na Android aplikace vypadá vyladěně. Na stranu druhou jsou zde značně omezeny možnosti rozšířit aplikaci např. na stolní počítač. Dále je také vhodná na běžného uživatele, nastavení a ovládaní aplikace je mnohem jednodušší než u CSipSimple. Stačí nainstalovat, vložit vlastní telefonní číslo a volat. Nevýhodou je, že architektura systému je méně viditelná. Otázka zabezpečení je však vždy těžká. A proto budu u všech aplikací předpokládat, že tvůrci opravdu nemají přístup k datům uživatelů.

3.7 Měření Ostel – WIFI

3.7.1 Spojení mobilní telefon - notebook

V následující tabulce je zobrazeny informace o probíhajícím spojení mezi aplikací CSipSimple na mobilním telefonu a VoIP klientem Jitsi na notebooku.

Tabulka 3.4: *Naměřené hodnoty spojení - Jitsi*

Přenos signalizace	Lokální IP	Cílová IP	Loss rate [%]
TLS	192.168.1.3	66.151.32.200	0 / 0
Bandwidth		Jitter	
Downlink [Kbps]	Uplink [Kbps]	Downlink [ms]	Uplink [ms]
14	32	15	7
RTT [ms]	Typ spojení	Transportní protokol	Šifrování
566	UDP	ZRTP	AES – 128 bit

Cílová IP adresa 66.151.32.200 odpovídá serveru umístěnému v USA, Miami. Vzdálenost a relativně vysoký počet průchozích routerů (více jak 15 HOPů) může být hlavní důvod, proč je během přenosu zaznamená tak vysoké RTT. Zpoždění více jak půl sekundy, může být u realtime komunikace problém. Může se zde projevovat vysoké zpoždění mezi volajícími a tím zhoršit kvalitu hovoru.

Vzhledem k typu spojení – směrové bezdrátové připojení, vysoká hodnota RTT mohla být způsobena aktuálními povětrnostními podmínkami. Toto je u WIFI běžný jev a prakticky nelze eliminovat.

Co se týče samotného testovacího hovoru, přes vysoké RTT během hovoru, bylo zpoždění hovoru nevýrazné a nijak citelně nesnižovalo kvalitu hovoru. Subjektivní hodnota **MOS: 3-4**.

3.7.2 Spojení mobilní telefon – mobilní telefon

V samotném měření oproti předchozímu měření nejsou z hlediska přenosu žádné podstatné rozdíly pro použití stejné metody přenosu dat. Spojení mobilní telefon – mobilní telefon probíhá instalací CSipSimple na obě zařízení. Přestože jsou obě zařízení na stejné sítí, spojení je navázáno skrze vzdálený server viz cílová IP a z toho serveru k příjemci hovoru.

3.8 Měření Ostel – HSPA+

3.8.1 Spojení mobilní telefon – mobilní telefon

Při měření skrze datové sítě T-Mobile spojení vykazovalo relativně dobrou hodnotu RTT. Doba odezvy do 200ms je dostačující a přibližně může odpovídat očekávané odezvě u této technologie přenosu. Oproti spojení skrze domácí WIFI síť tak tento druh spojení vykazuje lepší předpoklady ke kvalitnímu hovoru.

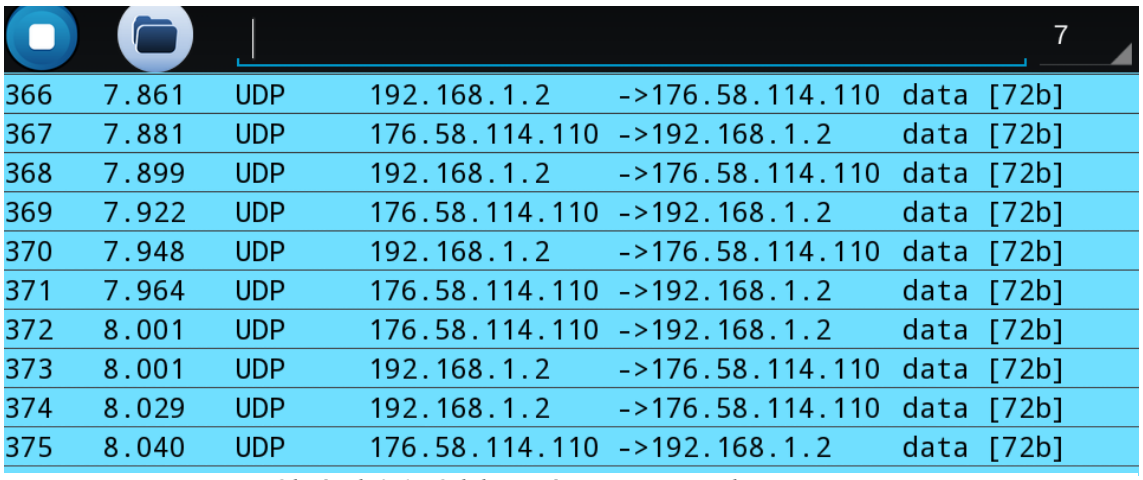
Tabulka 3.5: *Naměřené hodnoty spojeni T-Mobile*

Přenos signalizace	Lokální IP	Cílová IP	Loss rate [%]
TLS	37.48.32.23	66.151.32.200	0 / 0
Bandwidth		Jitter	
Downlink [Kbps]	Uplink [Kbps]	Downlink [ms]	Uplink [ms]
23	26	nezjištěn	nezjištěn
RTT [ms]	Typ spojení	Transportní protokol	Šifrování
183	UDP	ZRTP	AES – 128 bit

U druhého měření skrze mobilní připojení byla zaznamenáno nižší RTT, rychlost přenosu samotná zde byla podobná a při datovém toku do 30Kbps však nijak důležitá. Přestože se zde očekávaly spíše negativní výsledky, hovor byl čistý, bez zpoždění. Subjektivní hodnota **MOS: 5**

3.9 Měření RedPhone – WIFI

Měření RedPhone aplikace byla o poznání těžší důvodu toho, že na rozdíl od řešení Ostel funguje pouze na **platformě Android**. Proto možnosti měření se omezovaly pouze na aplikace dostupné z Google Store. V praxi tak měření probíhalo tak, že prvním krokem bylo navázat spojení mezi 2 koncovými stanicemi – 2 mobilními telefony. Tento provoz byl odchycen pomocí aplikace podobné Wireshark.



Obrázek 3.1: Odchycený UDP provoz, host - server

Na základě tohoto logu lze zjistit, skrze jaký server komunikace procházela. Skrze server na adrese 176.58.114.110 tak probíhala veškerá komunikace mezi oběma účastníky. Na základě tohoto lze poté server trasovat a poté zjistit přibližnou odezvu serveru.

Po trasování serveru bylo zjištěno, že server je umístěn ve Velké Británii, v Londýně. Průměrná naměřená hodnota odezvy byla 44ms bez kolísání a výpadků. Tato hodnota je pro VoIP velmi dobrá a kvalita spojení by tak měla být vysoká. Naopak při pokusu o zachycení provozu mezi mobilním telefonem a serverem se projevila lehce vyšší režie přenosu oproti Ostel. Jedná se přibližně o 52kbps při uplinku. To může být způsobeno použitím rozdílného kodeku. RedPhone používá na rozdíl od Ostel Speedx kodek.

Uskutečněný hovor byl čistý, bez zpoždění, oproti předchozí aplikaci však celkově kvalitnější. Subjektivní hodnota **MOS: 5.**

3.10 Měření RedPhone – HSPA+

Měření skrze mobilní datové sítě probíhalo obdobně. Na základě IP adresy serveru byla naměřena odezva a staženy testovací data. Na tomto testu, kdy bylo staženo několik megabytu dat, byl zaznamenán přibližně 6.38% packet lost. Při samotném testovacím hovoru se však neprojevily žádné nedostatky. Subjektivní hodnota **MOS: 5.**

	Minimum	Average	Maximum
RTT [ms]	61	133	1009
Downlink [Mbps]	1.86	4.71	8.97
Loss rate [%]	///	6.38	///

Tabulka 3.6: *Naměřené hodnoty RedPhone - HSPA+*

4 Závěrečné srovnání aplikací

V první řadě se jedná o velmi podobné aplikace. Obě fungují na stejném principu. Obě služby fungují relativně spolehlivě, jak se od freeware aplikací očekává. Přestože jsem se řešení od Ostel věnoval delší dobu, více se mi zalíbila aplikace od Open Whisper Systems, RedPhone.

Jak bylo na minulých stránkách řečeno, RedPhone poskytuje mnohem vetší uživatelský komfort, a dovolil bych si tvrdit, že se dokáže rovnat komerčním aplikacím. Neobtěžuje zbytečnými dotazy, vše se děje na pozadí. Uživateli tak stačí pouze vytočit telefonní číslo. To přičítám hlavně tomu, že RedPhone je pouze pro platformu Android. Vývojáři se tak mohli soustředit na jednu věc a tu zvládnout perfektně.

Na straně druhé je zde Ostel. Toto řešení ztrácí a získává svoji multiplatformností. Umožňuje šifrované spojení napříč platformami, ale neexistuje aplikace dělaná ryze pro Ostel určená pro uživatele – amatéry. Je zde mnoho programů podporující protokol, avšak každý vypadá jinak a tak budí dojem studentského projektu. Základní nastavení spočívá v několika relativně jednoduchých krocích, ale běžný uživatel nechce nastavovat nic. Chce nainstalovat a volat. V tomto aspektu tak jasně vyhrává RedPhone. Vzhledem k tomu, že obě fungují dobře, úroveň zabezpečení je prakticky na stejné úrovni, RedPhone tak vyhrává díky své jednoduchosti a praktičnosti.

Poslední odstavec bych rád věnoval řešení od firmy Probin, kterému jsem se věnoval v 2. kapitole. Pokusil jsem se zde nastínit, jak funguje jejich systém, a na základě informací, které byly volně dostupné, jakožto u komerčního produktu, jsem došel k názoru, že se prakticky nijak neliší od bezplatných řešení. Webové stránky firmy Probin jsou plné obrázků znázorňující funkci systému, které můžou neznalého uživatele zaujmout. Faktem však je, že toto řešení má podobně silné šifrování a stejně tak má problémy s šifrováním mezi uživatelem šifrovací aplikace a běžným volajícím. Jediný rozdíl tak vidím v ceně. Zatím co Probin vyžaduje za své služby téměř statisícovou částku, jsou zde velmi podobné služby zadarmo.

Závěr

Cílem práce bylo především najít možnosti jak bezplatně provádět šifrované hovory mezi uživateli mobilních telefonů na platformě Android. Této kategorii odpovídaly především 2 volně dostupné řešení a to Ostel a RedPhone. Tyto aplikace byly následně podrobeny testování kvality hovoru na několika různých zařízeních a datových připojení. Na základě měření a celkového subjektivního dojmu byly aplikace porovnány. V tomto porovnávání lehce vítězí aplikace RedPhone od Open Whisper Systems pro svůj celkově profesionálnější dojem. Obě aplikace však dosahují vysoké úrovně šifrovaní a lze obě doporučit k dalšímu užití.

Během získávání informací o způsobu šifrování aplikací vyvstal problém s ověřením pravosti uvedených informací. Přestože aplikace avizují určitou úroveň zabezpečení, nikdo z uživatelů nevidí do daného systému a nemůže si být 100% jist, že jeho data nemohou zneužita. Tento problém by mohl být zajímavým námětem na další zpracování.

Při průzkumu jsem také narazil na komerční řešení šifrování. V práci jsem se konkrétně věnoval systému od firmy Probin. Jedná se o velmi podobný systém jako u předchozích aplikací. Velmi užitečná by byla práce zabývající se detailními rozdíly právě mezi těmito řešeními z hlediska poměru cena/výkon.

Závěrem bych rád uvedl dnešní trend v bezpečnosti v mobilních sítích. Jak bylo v práci uvedeno, původní GSM síť již dávno neposkytuje kvalitní možnosti zabezpečení přenášených dat. Proto všechny 3 předešlé varianty tento problém obcházejí pomocí VoIP a vlastní implementace šifrování. Spojení s účastníky běžné telefonní sítě je tak stále nezabezpečeným spojením a může být zneužito.

Použitá literatura

[1] Enigma machine. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-03-22].
Dostupné z: http://en.wikipedia.org/wiki/Enigma_machine

[2] Cryptography. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-03-22].
Dostupné z: http://en.wikipedia.org/wiki/Cryptography

[3] *Crypto Corner* [online]. 2013 [cit. 2015-04-26].
Dostupné z: http://crypto.interactive-maths.com/

[4] Substitution cipher. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-04-26].
Dostupné z: http://en.wikipedia.org/wiki/Substitution_cipher

[5] Transposition cipher. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-04-26].
Dostupné z: http://en.wikipedia.org/wiki/Transposition_cipher

[6] Symmetric-key algorithm. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-04-26]. Dostupné z: http://en.wikipedia.org/wiki/Symmetric-key_algorithm

[7] GSM sítě napadnutelné útokem umožňujícím útočníkovi zneužít telefon. *Lupa.cz* [online]. 2011 [cit. 2015-04-26]. Dostupné z: http://www.lupa.cz/clanky/gsm-site-napadnutelne-utokem-umoznujicim-utocnikovi-zneuzit-telefon-cekam-na-operatory/

[8] PROKEŠ, Martin. *Bezpečnostní problémy GSM*. Ostrava, 2014. Dostupné z: http://hdl.handle.net/10084/103798. Diplomová práce. Vysoká škola báňská - Technická univerzita Ostrava. Fakulta elektrotechniky a informatiky. Vedoucí práce Vozňák Miroslav.

[9] Subscriber identity module: SIM card. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-03-22].
Dostupné z: http://en.wikipedia.org/wiki/Subscriber_identity_module

[10] SIM Cards. In: *Forensics Wiki* [online]. 2014 [cit. 2015-04-26]. Dostupné z: http://www.forensicswiki.org/wiki/SIM_Cards

[11] Session Initiation Protocol. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-04-26]. Dostupné z: http://en.wikipedia.org/wiki/Session_Initiation_Protocol

[12] ZRTP. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-03-30].
Dostupné z: https://en.wikipedia.org/wiki/ZRTP

[13] RFC 6189. *ZRTP: Media Path Key Agreement for Unicast Secure RTP*. Internet Engineering Task Force, 2011.
Dostupné z: https://tools.ietf.org/html/rfc6189

[14] *Probin* [online]. © 2008-2015 [cit. 2015-04-26].
Dostupné z: http://www.probin.cz/

[15] *The Guardian Project* [online]. © 2015 [cit. 2015-04-26]. Dostupné z: https://guardianproject.info/

[16] Orweb: Private Web Browser. *The Guardian Project: Mobile Apps and Code You Can Trust* [online]. 2015 [cit. 2015-03-22].
Dostupné z: https://guardianproject.info/apps/orweb/

[17] MIČKA, Pavel. Transpoziční šifra. *Algortitmy.net: příručka pro vývojáře* [online]. 2008 - 2015 [cit. 2015-03-13].
Dostupné z: http://www.algoritmy.net/article/51/Transpozicni-sifra

[18] Orbot: Mobile Anonymity + Circumvention. *The Guardian Project: Mobile Apps and Code You Can Trust* [online]. 2015 [cit. 2015-03-22].
Dostupné z: https://guardianproject.info/apps/orbot/

[19] *Open WhisperSystems* [online]. 2013-2014 [cit. 2015-03-22].
Dostupné z: https://whispersystems.org/

[20] ChatSecure: Private Messaging. *The Guardian Project: Mobile Apps and Code You Can Trust* [online]. 2015 [cit. 2015-03-22].
Dostupné z: https://guardianproject.info/apps/chatsecure/

[21] *Ostel: Encrypted Phone Calls* [online]. 2015 [cit. 2015-03-22].
Dostupné z: https://ostel.co/

[22] GSM. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-03-22].
Dostupné z: http://en.wikipedia.org/wiki/GSM

[23] A5/1. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2015-03-22].
Dostupné z: http://en.wikipedia.org/wiki/A5/1

[24] *Tor Project: Anonymity Online* [online]. [cit. 2015-03-22].
Dostupné z: https://www.torproject.org/

[25] RedPhone: Architecture Overview. *Gitgub.com* [online]. 2013 [cit. 2015-04-27].
Dostupné z: https://github.com/WhisperSystems/RedPhone/wiki/Architecture-Overview